Unsere Daten: Was verraten sie über uns?

Dass unsere Daten gesammelt werden, dürfte inzwischen hinlänglich bekannt sein. Aber was danach mit diesen Daten passiert, an wen sie weitergegeben werden und welche Schlussfolgerungen daraus gezogen werden, von all dem haben die meisten Menschen keine Vorstellung. Die nachfolgenden Abschnitte widmen sich diesem Aspekt der Sammlung von Daten.

Nothing to Hide

> »Ich habe nichts zu verbergen.«
> »Nothing to Hide.«[1]

»Ich habe nichts zu verbergen« ist wohl die am meisten verbreitete Ausrede, warum Privatheit unwichtig sei.

Als Begründung für die Unsinnigkeit dieser Aussage wird gerne eine Aussage von Richelieu zitiert: »Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen.«[2]

Häufig lassen eine gewisse Bequemlichkeit sowie der Komfort der vielen kostenlosen Dienste, die das Leben einfacher und bequemer machen und auf deren Nutzung man nicht verzichten möchte, die Ri-

1 Titel eines Buches von Daniel Solove. Ders. 2001.

2 Schneier 2006a; vgl. die engl. Fassung Schneier 2006b.

siken einer Herausgabe von privaten Daten als marginal erscheinen. Immer wieder findet man Berichte, dass Menschen sehr sensible private Daten bereitwillig gegen marginale Belohnungen herausgeben.

> »Ein Gratis-Mandelgipfel genügt als Köder, und schon reichen zahlreiche Kunden einem unbekannten Bäcker AHV-Nummern [Sozialversicherungsnummern] und Angaben zu Partnerschaften über die Theke.«[3]

Gerne wird auch argumentiert, dass man, wenn man nichts Unrechtes getan habe, man auch nichts zu verbergen brauche, was impliziert, dass Privatheit das Verbergen von Unrecht zum Ziel hat. Das ist ein vielfach angeführtes Argument, um Vertreter des »Nothing to Hide« Standpunktes zu überzeugen.

Doch mag man noch so gute Argumente haben, die Menschen, die den Standpunkt vertreten, sie hätten nichts zu verbergen, sind weitgehend argumentations- und überzeugungsresistent. Alle Versuche, sie zu überzeugen, sind damit von vornherein zum Scheitern verurteilt – egal wie gut die vorgebrachten Argumente sind.

Man kann das sehr schön an der Reaktion auf die Snowden-Enthüllungen sehen. Eine repräsentative Umfrage des Marktforschungsunternehmens GfK im Auftrag der »Welt am Sonntag« zeigt, dass 76,9 Prozent der Befragten ihren Umgang mit persönlichen Daten nicht geändert haben.[4]

Interessant ist, was der Philosoph Michael Sandel in diesem Zusammenhang über seinen Sohn sagt:

> »Der ist erst Ende 20 und ihm ist es egal, ob die NSA erfährt, mit wem er telefoniert hat. Denn für ihn liegt die Grenze ganz woanders: Wenn seine Eltern auf solche Informationen zugreifen könnten, würde er es als Verletzung seiner Rechte sehen.

3 Mäder 2019.

4 Vgl. Heuzeroth 2014.

> Das Beispiel zeigt, dass es bei der Frage nach Privatsphäre eine Rolle spielt, wer solche Daten nutzen möchte und ob es mit einer Zustimmung geschieht.«[5]

Wer weiß schon, welche Daten über ihn gesammelt werden. Wer sich dafür interessiert, wird in Publikationen eine Fülle von Hinweisen finden. Damit kann er zumindest eine Ahnung bekommen, was über ihn gesammelt sein könnte, auch wenn es im Detail nicht feststellbar ist. Dieses Datensammeln ist im Grunde heimtückisch. Man merkt es nicht, es tut nicht weh, und sollte es wirklich wehtun, ist es zu spät. Man spricht hier auch von der mangelnden Spürbarkeit von Überwachung.[6]

Ein weiterer Punkt ist, dass kaum jemand eine Vorstellung hat, was man mit diesen Daten machen kann, welche Informationen sich daraus gewinnen und welche Schlussfolgerungen sich ziehen lassen.

So wird häufig die Ansicht vertreten, dass die sogenannten Verbindungsdaten, also wer, wann mit wem kommuniziert hat, unkritisch seien. Amerikanische Forscher haben jedoch in einer Studie nachgewiesen, dass die Überwachung mittels dieser Verbindungsdaten (auch als Telefonmetadaten bezeichnet) erhebliche Auswirkungen auf die Privatsphäre hat. Telefonmetadaten sind eng miteinander verbunden, leicht wiedererkennbar und ermöglichen auf einfachste Weise Zugang zu Orten, Beziehungen und sensiblen Schlussfolgerungen.[7]

Dem Thema »Privacy« hat der amerikanische Juraprofessor an der George Washington University Law School, Daniel Solove, ein sehr lesenswertes Buch gewidmet. Es hat den Titel »Nothing to Hide«[8]. Ob er damit wirklich eine größere Gruppe überzeugen konnte, darf man bedauerlicherweise bezweifeln.

---

5 Wir brauchen eine neue Privacy-Debatte, 2016.

6 Vgl. Jahr 1 nach Snowden, 2015.

7 Vgl. Mayer/Mutchler/Mitchel 2016.

8 Solove 2001.

Hinzu kommt ein weiterer Aspekt: Es gibt inzwischen ein Phänomen, das mit dem Begriff der »Inverse Privacy« beschrieben wird.

> »Eine persönliche Information, zu der jemand Zugang hat, aber Du selbst nicht, bezeichnet man als inversely (entgegengesetzt) privat.«[9]

Damit wird die Situation beschrieben, dass eine dritte Partei Zugriff auf meine privaten Daten hat, ich selbst diesen Zugriff aber nicht habe.

Besonders brisant ist das, wenn die gespeicherten Daten einer Analyse unterzogen werden. Welche Schlüsse über meine Kreditwürdigkeit, meinen Gesundheitsstatus und über vieles mehr gezogen werden, erfahre ich nicht, habe somit auch keine Möglichkeit, etwaige Fehler zu korrigieren.

Es ist diese Inverse Privacy, die wir immer häufiger antreffen. Ein anschauliches Beispiel dafür bietet Max Schrems, dem Facebook nach langwierigem Verfahren eine CD mit 1200 pdf-Seiten zur Verfügung stellte. Dies war die Antwort auf eine Anfrage von Max Schrems nach allen Daten, die Facebook über ihn gespeichert hat.[10]

> »Wenn wir unsere Daten einfach gratis weggeben, vergeben wir auch ein Teil unserer Stimme in der Demokratie.«[11]

Inzwischen weiß man, dass diese Daten auch dazu benützt werden, Menschen zu beeinflussen. Das bekannteste Beispiel dafür ist Cambridge Analytica. Diese Firma hat mit (nicht rechtmäßig erworbenen) Daten von Facebook-Nutzern versucht, die Wahl von Donald Trump sowie den Brexit zu unterstützen. Ob diejenigen, die so leichtfertig

9 »Call an item of your personal information inversely private if some party has access to it but you do not.« (Gurevich/Hudis/Wing 2016)

10 Vgl. Bähr 2015; Levine 2015.

11 Pagel/Portmann/Vogt 2020.

ihre Daten zur Verfügung stellen, sich darüber im Klaren sind, wozu ihre Daten missbraucht werden können, mag man bezweifeln.

No Place to Hide

> »Es wird keinen Ort mehr geben, wo man sich verstecken kann.«[12]

> »Siehst du, die Übeltäter [die Terroristen] schlagen gerne zu, und dann versuchen sie, sich zu verstecken. Und langsam, aber sicher, werden wir sicherstellen, dass sie keinen Platz zum Verstecken haben.«[13]

Diese Warnung des amerikanischen Präsidenten George W. Bush, dass es nirgendwo auf der Welt mehr einen Platz geben werde, wo man sich verstecken kann, richtet sich zunächst an Terroristen. Es war eine seiner Reaktionen auf den Anschlag vom September 2001 auf das World Trade Center.

Die Gefahren durch Überwachung wurden in den USA schon sehr früh erkannt. So warnte Senator Frank Church in einer Nachrichtensendung:

> »Diese Fähigkeit [der NSA alles zu überwachen] könnte zu jeder Zeit gegen das amerikanische Volk gerichtet werden, und kein Amerikaner hätte mehr Privatsphäre. […] Es gäbe keinen Platz mehr zum Verstecken.«[14]

---

12 Es gibt eine ganze Reihe von Büchern mit diesem Titel, z.B. Greenwald 2014.

13 »You see, the evildoers [the terrorists] like to hit and then they try to hide. And slowly, but surely, we're going to make sure they have no place to hide.« Bush at FEMA Headquarters, 2001.

14 »That capability [of the NSA] at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to

Bemerkenswert an diesem Zitat ist, dass diese Warnung vor den Möglichkeiten der NSA aus dem Jahr 1975 stammt (siehe Kapitel »Privatheit und Demokratie«). Senator Frank Church war Vorsitzender des Sonderausschusses des US-Senats zur Untersuchung des Regierungshandelns mit Bezug zu Aktivitäten der Nachrichtendienste. Aus diesem Sonderausschuss, auch als *Church Committee* bezeichnet, gingen die ständigen Ausschüsse zur Kontrolle der Nachrichtendienste im US-Senat und im Repräsentantenhaus hervor.[15]

Es gibt zwei wichtige Bücher mit identischem Titel, die sich mit dem Verlust der Privatsphäre durch die massenhaften Datensammlungen befassen.

1. »No Place to Hide« von Robert O'Harrow Jr., 2006[16]

O'Harrow zeigt uns, dass es in dieser neuen Welt eines hochtechnologisierten Inlandgeheimdienstes buchstäblich keinen Platz zum Verstecken gibt.[17] Dieses Buch hat an seiner Aktualität kaum etwas eingebüßt.

Die Datenindustrie wird weiter und immer schneller Informationen über uns sammeln. Die Regierung wird diese Daten im Namen des Heimatschutzes und der Strafverfolgung kaufen. Vermarkter werden uns weiterhin beobachten und Profile erstellen, um uns noch profitabler für sie zu machen.[18]

---

monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide.« Bamford 2005.

15 Vgl. Church Committee 2019.

16 O'Harrow Jr. 2006.

17 »O'Harrow shows us that, in this new world of high-tech domestic intelligence, there is literally no place to hide.« No Place to Hide 2006.

18 »The data industry continues to collect information about you at an accelerating pace. The government continues to buy it in the name of homeland security and law enforcement. Marketers continue to watch you and profile you with the aim of making you more profitable to them.« O'Harrow Jr. 2006, S. 303-304.

Daran hat sich bis heute nichts geändert. Die Snowden-Enthüllungen zeigen im Detail das, was O'Harrow bereits 2006 beschrieben hat.

2. »No Place to Hide« von Glenn Greenwald, 2014[19, 20]

Tatsächlich trifft die Warnung, dass es nirgendwo auf der Welt mehr einen Platz geben werde, wo man sich verstecken kann, inzwischen auf jeden zu, d.h. in unserer Zeit wird niemand mehr die Möglichkeit haben, sich zu verstecken. Man mag sagen, verstecken müssen sich nur Terroristen und Kriminelle, aber kein ehrenwerter Bürger. Doch sollte man nicht vergessen, dass die Möglichkeit, sich zu verstecken z.B. indem man in den Untergrund ging, vielen während der Herrschaft des Naziregimes das Leben gerettet hat. Damals war das noch möglich. Heute spricht viel dafür, dass ein Verstecken nicht mehr möglich ist.

> »Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun.«[21]

Dieser sehr bekannte Ausspruch von Google CEO Eric Schmidt zeigt in erschreckender Weise, dass hier eine Welt propagiert wird, in der man sich nicht nur nicht mehr verstecken kann, sondern in der es zudem keine Geheimnisse mehr gibt.

19 Greenwald 2014.

20 Greenwald 2015, Titel der deutschen Ausgabe: *Die globale Überwachung: Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen*.

21 Stöcker 2009. »If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.« Esguerra 2009.

Wir werden überwacht

> »Du wirst beobachtet.«[22]
>
> »Überwachung ist das Geschäftsmodell des Internet.«[23]
>
> »Einen Staat, der mit der Erklärung, er wolle Straftaten verhindern, seine Bürger ständig überwacht, kann man als Polizeistaat bezeichnen.«[24]

Regierungsbehörden und Privatunternehmen wissen sehr viel über uns. Sie wissen, wo wir leben, was wir verdienen, wofür wir unser Geld ausgeben, was uns gefällt, wofür wir uns interessieren, was wir lesen usw. Die Liste lässt sich beliebig fortsetzen. Es gibt kaum etwas, was sie nicht wissen.

Dabei ist nicht entscheidend, ob staatliche Stellen oder Konzerne die Daten sammeln. Denn im Zweifelsfalle kann sich der Staat die Informationen von den Konzernen besorgen. Insbesondere in den USA müssen die großen Konzerne auf Grund des Patriot Acts die gesammelten Daten der Regierung auf Anforderung zur Verfügung stellen.

»Solange Überwachung das Geschäftsmodell des Internets ist, gibt es keinen großen Unterschied zwischen den Regierungen und den Konzernen«, sagt Bruce Schneier, »›sie alle wollen dich ausspionieren‹.«[25]

---

22 »You are being watched.« O'Harrow Jr. 2006.

23 »Surveillance is the business model of the Internet.« Schneier 2015.

24 Ernst Benda, ehemaliger Präsident des Bundesverfassungsgerichts, im Interview mit tagesschau.de, 5. Juni 2007, Stegers 2007.

25 »Solange Überwachung das Geschäftsmodell des Internets ist, gibt es keinen großen Unterschied zwischen den Regierungen und den Konzernen, … sie alle wollen dich ausspionieren.« (nach Schneier) Drösser 2016.

> »Wer sieht, kann kontrollieren; wer gesehen wird, kann kontrolliert werden.«[26]

Seit Snowden wissen wir, wie die Internetüberwachung der Geheimdienste, insbesondere der NSA funktioniert. Es sind die Hauptknotenpunkte der Kabel- und Servicewerke sowie die IXPs [Internet-Knoten], an denen so gut wie alle Kommunikation abgefangen werden kann. Zudem verschafft die NSA sich Zugriff auf die Server der großen Internetkonzerne, die die vertraulichen Daten ihrer Kunden dort speichern. So gelingt es ihr ein zentralisiertes Schattennetzwerk zu erschaffen, mit dem sie das gesamte globale Netzwerk übersieht und letztendlich auch kontrolliert. Dies alles geschieht unter Ausschaltung jeglicher demokratischen Kontrolle und unbemerkt für die Nutzer des Netzes.

> »Zumindest in der Theorie kann die NSA so nun Informationen über jede normale Internetteilnehmerin abrufen, die Kommunikation jeder mit jeder heimlich mitlesen oder sogar Kommunikationsströme einfach abbrechen oder unbemerkt manipulieren.«[27]

Wer auch immer Daten sammelt, der wird diese Daten nicht nur sammeln, sondern eben auch analysieren. Und das läuft völlig intransparent für den Nutzer ab, d.h. er hat keine Ahnung, welche Schlüsse aus seinen Daten gezogen werden. Die Daten werden bewertet und klassifiziert. Dabei geht es nicht nur darum, auf welche Werbung jemand besonders anspricht, sondern es kann durchaus sein, dass damit der Preis bestimmt wird, den jemand angeboten bekommt, aber auch die Sonderangebote, die gemacht werden. Ob jemand einen Handyvertrag oder einen Kredit bekommt, wie teuer eine Versicherung sein wird,

26 Nosthoff/Maschewski 2017.

27 Fichtner 2016.

die er abschließen möchte und dergleichen mehr, all dies ergibt sich u.a. aus der Analyse seiner Daten.

Wer weiß schon, dass man aus ca. 170 Likes auf Facebook auf sehr sensible Daten schließen kann wie ethnische Zugehörigkeit, Geschlecht, sexuelle Orientierung, politische Präferenzen, religiöse Einstellung, Raucher bzw. Nichtraucher, Trinker, Einnahme von Drogen, Alleinstehend oder in einer Partnerschaft lebend?[28]

> »Bei der Überwachung geht es nicht darum, Ihre Geheimnisse zu kennen, sondern um die Verwaltung von Bevölkerungsgruppen, die Verwaltung von Menschen.«[29]

> »Menschen ändern automatisch ihr Verhalten, wenn sie überwacht werden.«[30]

Das ist der Fall, wenn ein Versicherungsunternehmen, wie z.B. Generali, Kunden mit einer ermäßigten Krankenversicherung lockt, wenn sie per App belegen, dass sie Sport treiben. De facto ist dies eine Zustimmung zur Überwachung mit dem Ziel einer Verhaltensänderung im Lebensstil. Der Betroffene gibt damit ein Stück seiner Freiheit auf, indem er versucht, sich so zu verhalten wie der Konzern es wünscht. Was man dabei nicht übersehen sollte, ist, dass es hier keineswegs um das Wohl des Einzelnen geht, sondern einzig und allein um die ökonomischen Interessen von mächtigen Konzernen. Wenn der Betroffene alt oder krank wird, kann man davon ausgehen, dass sich das Belohnungssystem gegen ihn wenden wird.[31]

---

28 Vgl. Christl/Spiekermann 2016, S. 15.

29 »Surveillance is not about knowing your secrets, […] but about managing populations, managing people.« Grossman 2016.

30 Janker 2014.

31 Vgl. ebd.

> »Das größte Sicherheitsrisiko ist aber immer noch der sorglose Umgang der Bürger mit ihren persönlichen Daten.«[32]

Es ist dieser Aspekt, der der Überwachung Tür und Tor öffnet. Selbst wenn Bürger sagen, dass ihnen ihre Privatsphäre wichtig ist, richten sie sich nicht danach. Man spricht hier vom sogenannten Privacy Paradox.

> »Das Privacy Paradox beschreibt die – auf den ersten Blick – widersprüchliche Tatsache, dass sich Internetnutzer einerseits Sorgen um ihre Privatsphäre im Netz machen, andererseits aber ganz und gar nicht besorgt handeln: Trotz großer Bedenken stellen sie sensible Daten wie Handynummern, Aufenthaltsorte oder private Fotos offen ins Netz. Das Privacy Paradox umfasst dieses Auseinanderdriften von Einstellungen und konkretem Handeln in der digitalen Welt.«[33]

Das Internet der Dinge (IoT)

> »Dinge aus unserem Alltag sammeln Daten über uns, verschicken diese und werten sie aus.«[34]

Das Internet der Dinge (Internet of Things) besteht aus minimalen Sensoren und Minicomputern, die untereinander im Informationsaustausch stehen. Sie sind so klein, dass sie überall eingesetzt werden können, in Geräten, in Bekleidung und sogar im menschlichen Körper. Sie sind mit dem Internet verbunden und können so kommunizieren. Sie sammeln Unmengen an Daten, analysieren sie und geben sie weiter. Dieses Internet der Dinge ist ein riesiges globales Netzwerk,

32 Thiel 2016.

33 Lutz/Strathoff 2014.

34 Dr. Datenschutz 2015.

dessen Struktur ›jederzeit und überall verfügbar, für jedes und jeden‹ ist. Es verbindet Geräte, Systeme, Daten und Personen. Man spricht auch davon, dass dieses Netzwerk ubiquitous – allgegenwärtig – ist. Dadurch eröffnen sich bisher ungeahnte Möglichkeiten z.B. zur technischen Steuerung von Geräten, die den Alltag der Menschen gravierend verbessern. Man denke nur daran, wie bequem es ist, wenn man mit dem Handy auf dem Nachhauseweg die Heizung hochstellen kann, oder wenn der Staubsauger eine Info an das Handy sendet, dass neue Staubsaugerbeutel bestellt werden müssen. Weitere Beispiele sind – die Waschmaschine, die an das Handy eine Nachricht schickt, wenn sie durchgelaufen ist – oder das Fitnessarmband, das die sportlichen Aktivitäten seines Trägers misst und diese auf sein Handy schickt, vielleicht aber auch an seine Krankenkasse – oder das mit vielen Sensoren und Prozessoren ausgestattete Auto, das die Strecke erfasst, die gefahren wurde, und das mitteilt, wenn getankt werden muss, und vieles mehr – oder der Fernseher, der nicht nur den Aufruf von TV-Sendungen erlaubt, sondern mit dem man Zugriff auf Online-Videotheken hat, mit dem man im Internet surfen und auch per Skype kommunizieren kann – oder der Kühlschrank, der erkennt, wann welche Waren verbraucht sind und diese selbstständig nachbestellt. Ein gutes Beispiel ist auch die französische Bahn, die Züge und Gleise mit Sensoren ausrüstet, die Daten für die Wartung senden. Das ermöglicht den Ingenieuren in den Reparaturwerkstätten, frühzeitig Probleme zu erkennen und Ersatzteile zu bestellen, noch bevor ein Defekt auftritt.[35] Die Liste ließe sich beliebig fortsetzen.

Dass, wie bei allem Neuen, mit dieser Technologie auch Gefahren verbunden sind, gerät dabei oft in Vergessenheit.

35 Vgl. Hill 2018.

> »Daten, die aus dem Internet der Dinge gesammelt werden, decken sensible Verhaltensmuster auf, die Verbraucher lieber geheim halten würden.«[36]

Auf diese Risiken für die Privatsphäre weist das Electronic Privacy Information Center in den USA hin. Bei der Vielzahl der Daten und Kommunikationsbeziehungen gestaltet sich deren Schutz immer schwieriger. So mag der intelligente Stromzähler (Smart Meter), der den Stromverbrauch misst und gegebenenfalls an den Versorger sendet, beim Stromsparen helfen. Mit ihm lässt sich aber auch feststellen, wie viele Menschen gerade in der Wohnung sind und was sie tun.[37] Jemanden in einer Wohnung zu verstecken, ist damit kaum noch möglich. Man denke hier nur an Anne Franks Familie. Sie wäre bei Vorhandensein eines Smart Meters wohl sehr viel früher entdeckt worden.

Die Privatsphäre ist durch das Internet der Dinge auch dadurch bedroht, dass die riesige Menge der Daten ein sehr detailliertes Abbild der Realität erlaubt. Man kann mit Hilfe dieser vielen Sensoren das alltägliche Leben einer großen Zahl von Menschen in Echtzeit erfassen. Wer kann sich schon vorstellen, dass sich aus diesen Daten auch Rückschlüsse auf persönliche Vorlieben, Gewohnheiten, Krankheiten oder Stimmungen ziehen lassen.[38]

Ein typisches Beispiel für die Manipulation des Nutzers sind Telematik-Tarife von Kfz-Versicherungen. Bei diesen Tarifen entscheidet das Fahrverhalten über die Höhe der Versicherungsprämie. Der Versicherer kontrolliert damit nicht nur den Fahrstil des Versicherten, sondern er versucht außerdem, diesen dahingehend zu beeinflussen,

---

36 »Data Collected from the Internet of Things May Reveal Sensitive Behavior Patterns That Consumers Wish to Keep Private.« The On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things 2016.

37 Vgl. Biermann 2013.

38 Vgl Internet der Dinge Was ist das, was bringt das, wie riskant ist das? 2016. (test ist eine Zeitschrift der Stiftung Warentest)

dass weniger Unfälle verursacht werden, wodurch sich der niedrigere Versicherungstarif für die Versicherung letztlich auszahlt.

> »Immerhin behauptet die Allianz: Autofahrer, die diese App einsetzten, führen nach einiger Zeit deutlich vorsichtiger, es gebe einen signifikanten Einfluss des Systems auf den Fahrstil.«[39]

Wer hätte sich zudem vorstellen können, dass ein Herzschrittmacher oder ein Fitnessarmband zu Belastungszeugen bei schweren Verbrechen werden können.[40] Wer weiß schon, dass man den Fahrer eines Wagens durch die Analyse des Fahrstils eindeutig identifizieren kann. Damit lässt sich z.B. feststellen, ob der Sohn und nicht der Vater der Fahrer des Wagens war, oder ob der Fahrer unter Alkohol oder Drogen stand. Somit kann also auch das Auto zum Belastungszeugen gegen den Fahrer des Wagens werden.[41]

Dabei bleibt es aber nicht bei einer Analyse, sondern der nächste Schritt ist dann diese Realität zu kontrollieren.

> »Das Problem [das oft in Zusammenhang mit Ubiquitous Computing gesehen wird] ist die Beeinträchtigung der Privatsphäre. In Wirklichkeit sind es aber die Kontrollmöglichkeiten, die diese Technologie so problematisch machen.«[42]

Die Gefahr der Kontrolle durch solche allgegenwärtigen Systeme hat bereits der US-Informatiker Mark Weiser (1952 bis 1999) erkannt.[43]

---

39 Siedenbiedel 2017.

40 Vgl. Heller 2017.

41 Vgl. Greenberg 2016.

42 »The problem [associated with ubiquitous computing] while often couched in terms of privacy is really one of control.« Christl/Spiekermann 2016, S. 118.

43 »According to Mark Weiser: The problem, while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, whe-

Beispiele dafür in der heutigen Zeit z.B. sind das Fitnessarmband, das die körperlichen Aktivitäten seines Trägers überwacht, der Fernseher, der Auskunft geben kann über empfangene Sendungen, aber auch über die Anzahl der Personen im Raum. Ist die Spracherkennung aktiv, können sogar Gespräche aufgenommen werden.[44] Die elektrische Zahnbürste, deren App das Putzverhalten analysiert und Tipps gibt. Vernetzte Haushaltsgeräte und Sensoren, die zum Beispiel dabei helfen können, dass alte Menschen länger in ihren Wohnungen bleiben können, indem sie überwachen, ob sich ein Mensch normal in seiner Umgebung bewegt, und bei Problemen den Pflegedienst oder einen Verwandten alarmieren.[45]

Shoshana Zuboff warnt daher zu Recht vor diesen Gefahren des Internet der Dinge und kämpft gegen die Übermacht von Google:

> »Das Internet der Dinge bietet gewaltige Möglichkeiten zum Reality-Mining und zur Beeinflussung der Realität. […] Google und andere werden ihr Geld damit verdienen, dass sie diese Realität kennen, manipulieren, kontrollieren und in kleinste Stücke schneiden.«[46]

Bemerkenswert ist, dass bei einem ersten Projekt für ein Smart Home, der intelligenten Steuerung einer Wohnung oder eines Wohnhauses, dieses so konzipiert war, dass Daten aus diesem Projekt ausschließlich den Hausbewohnern zustanden, so dass der Schutz der Privatsphäre gewahrt blieb.[47]

Kaum jemand weiß, dass das auch heute noch möglich ist. Man kann nämlich ein Smart Home auch ohne Internet betreiben. »Wer

---

re information is flowing, how it is being used … and what are the consequences of any given action.« Chow 2017.

44 Vgl. Lobe 2017.

45 Vgl. Schipper 2015.

46 Zuboff 2014.

47 Vgl. Zuboff 2018, S. 20.

sein Smart Home offline lässt, ist sehr viel sicherer – muss aber auf einige Funktionen verzichten.«[48]

> »Es geht nicht mehr nur um Ihre Privatsphäre, sondern auch um Ihr Leben.«[49]

Auf möglicherweise tödliche Gefahren durch das Internet der Dinge weist Ross Anderson hin, ein renommierter Sicherheitsexperte und Professor an der University of Cambridge. So kann der Hackerangriff auf den Bordcomputer eines Autos einen tödlichen Unfall zur Folge haben. Ein gehackter Fernseher ist zwar nicht lebensgefährlich, aber den geplanten Fernsehabend dürfte man wohl erst einmal vergessen. Und was passiert, wenn ein Herzschrittmacher gehackt wird, mag man sich lieber nicht ausmalen.

Es gilt daher, bei den Nutzern ein Bewusstsein für das Vorhandensein dieser Datensammlungen und deren Risiken zu schaffen. Zudem stellt sich die Frage, ob wirklich alles mit jedem vernetzt sein muss. Auch wird das Thema Sicherheit dieser Systeme in Zukunft immer wichtiger werden.

Trotz aller Gefahren, sei es durch die Bedrohung der Privatsphäre als auch durch Möglichkeiten zur Kontrolle und zur Manipulation sowie gravierender Sicherheitsmängel, wird kaum jemand in unserer Gesellschaft mehr auf die bisher ungeahnten Möglichkeiten, die ein solches riesiges Netzwerk bietet, verzichten wollen.

48 Ohland 2019.

49 »It's not just your privacy that's on the line anymore, it's your life.« Anderson 2017.